Breakthroughs in Standardisation of IT Security Criteria

Eugene F. Troy
Project Manager, IT Security Criteria & Evaluations
National Institute of Standards and Technology
Gaithersburg, Maryland, USA

Background - Why the Common Criteria:

There are four main Driving Factors affecting the current activity in IT security criteria and product evaluations. These factors are all closely inter-related:

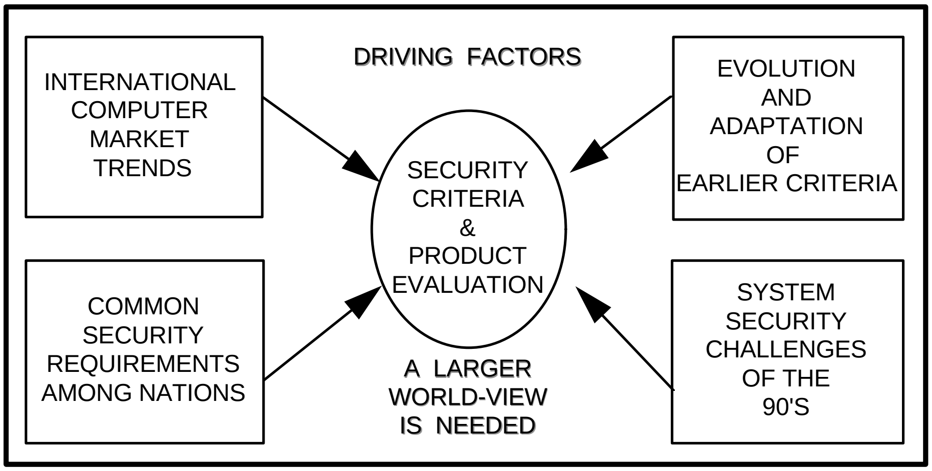
DRIVING FACTORS
INTERNATIONAL COMPUTER MARKET TRENDS
EVOLUTION AND ADAPTATION OF EARLIER CRITERIA
SECURITY CRITERIA & PRODUCT EVALUATION
COMMON SECURITY REQUIREMENTS AMONG NATIONS
SYSTEM SECURITY CHALLENGES OF THE 90'S
A LARGER WORLD-VIEW IS NEEDED

Figure 1: Rationale for Evolving to the Common Criteria

- International Computer Market trends.
  The notion of a "national IT product manufacturer" is no longer useful. Almost all manufacturers in all countries desire to sell into the international market and are typically based multi-nationally too. These manufacturers understandably have no particular desire to develop and sell numerous variants of their popular products to meet various national security restrictions or demands.
- The need for evolution and adaptation of earlier criteria.
  In the US, the Trusted Computer Security Evaluation Criteria (TCSEC), the so-called "Orange Book" was published by NSA in the early 1980's to establish the US government's military IT security requirements. The TCSEC has only six requirement sets, all for stand-alone operating systems, of which only four have been used to any great extent. None of them, when closely examined, addresses good commercial IT security requirements or the age of connectivity. The TCSEC

worked well to describe security requirements for stand-alone mainframes, and it has been difficult to translate into network and database terms. The Information Technology Security Evaluation Criteria (ITSEC), published in the early 1990's by the European Commission, is similarly limited in that it doesn't address the security functions needed, containing only requirements for the assurance aspect. The function sets mentioned in the ITSEC are mainly those from the old TCSEC, and are considered "examples".

- System security challenges of the 90's.
  This brings us to the challenges of the "real world" of today, that of distributed systems, the World Wide Web, the internet and intranet -- widespread connectivity and routine trans-national information flows. Distributed access, dispersed and cooperative work-patterns, the need for routine protection of information in transit -- all of these are today's IT security problems and are crucial to global society. Unsecured, they represent serious avenues for attack that can have widespread economic and social repercussions.
- Common security requirements among nations.
  As the Europeans' ITSEC project first demonstrated, when the "not-invented-here" (NIH) factor is removed, IT security requirements are rather standard no matter what nations are involved. Two predominate: military/intelligence requirements and civil/commercial requirements.

Therefore, a larger world-view is needed, represented by the work on a Common Criteria (CC) for IT Security that forms a solid basis for trust among nations about the IT security specification and evaluation work they do, permitting general understanding and mutual recognition of these efforts.

Security Concepts and Relationships:

One may ask, what is the value of IT security criteria and product/system evaluation -- why do we need to bear the extra cost and time needed to apply them? The argument that forms the basis for security criteria and evaluation is generally as follows:

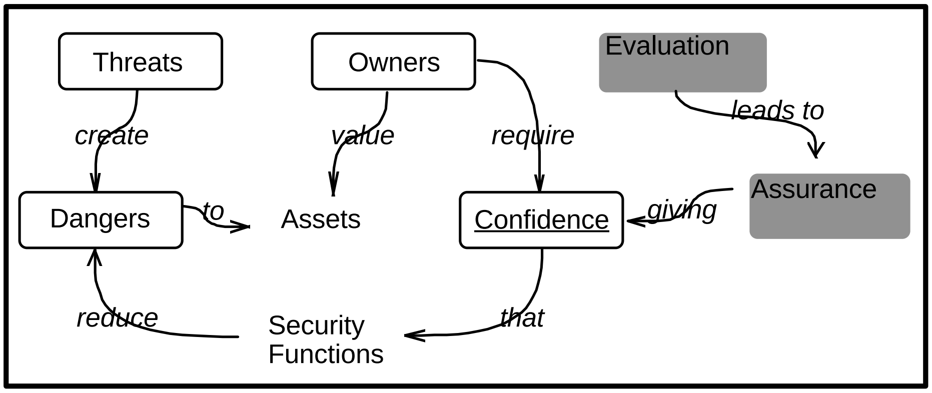

Figure 2: Security Concepts and Relationships

- Owners place some value on IT-based *assets*.
- *Threats* in the operating environment create *dangers* to these IT-based assets.
- Security features are applied to the operating environment and to the IT to reduce these known dangers (risk) to the assets. Those features which are incorporated into the IT are called *security functions* of the IT.
- However, owners expect and need to have some *confidence* that these embedded security functions in fact do the job needed and do it predictably. Otherwise, why bother with the added overhead and expense of including them?
- *Evaluation* of the security functions in the IT against accepted criteria leads to *assurance*, which gives the needed confidence in two ways: first that the security features are the right ones to meet the threats, and second that these security features are implemented appropriately, i.e., work predictably to do their job.

Twofold Purpose of IT Security Criteria:

IT security criteria help to provide the following two major benefits:

First, security criteria give a well-understood and common vocabulary and syntax for describing IT security requirements for product and systems. This requirements language can be viewed on two levels, as shown in the Common Criteria:

- The Protection Profile and Security Target constructs which first identify the relevant factors forming the basis for the IT security requirements, and then state those requirements in a standardised way that can be generally understood by both users and vendors.
- A catalogue of functional requirements that are complete enough to be useful in specifying security features for IT products and systems and are well-enough understood to be evaluatable.

Second, security criteria provide a solid technical basis for deciding to trust (i.e., have assurance about, have confidence in) the security functions in IT products and systems. This trust basis comes from performing a well-understood process of evaluating the IT product against a set of factors that are well-known to help provide this trust. These trust factors are expressed in the form of:

- A series of evaluation assurance levels, increasingly stringent 'packages' containing assurance requirements of various types which are known to work together in a mutually supportive way.
- A catalogue of all those individual assurance requirements comprising the assurance levels, plus others which could be specified additionally to help provide extra assurance as needed.

Context of IT Security Evaluations:

The complete context of IT security evaluation is represented by a number of factors related to product development.

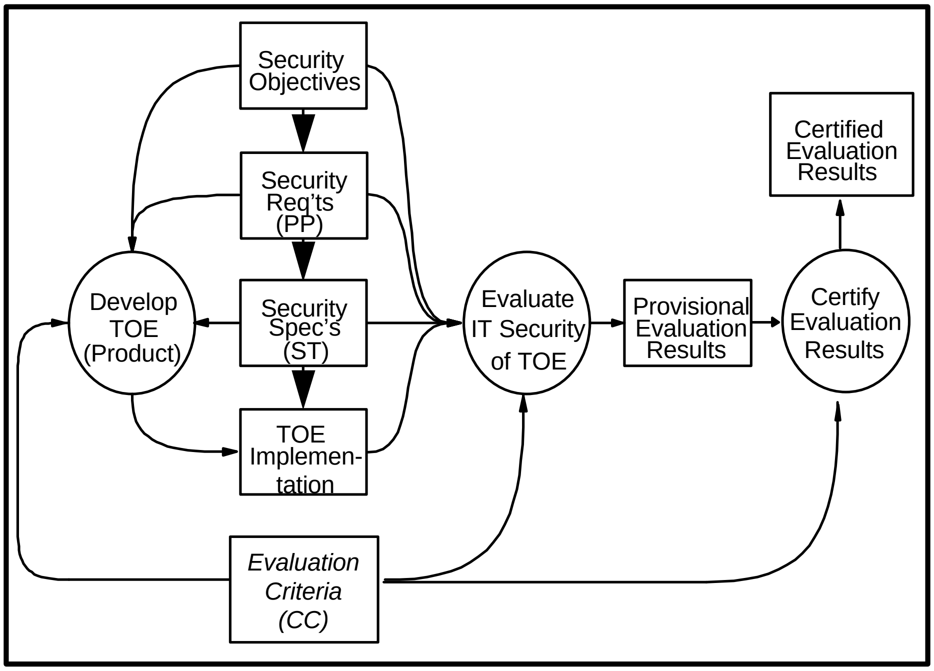

Figure 3: Context of IT Security Evaluations

During development, there is the increasingly specific instantiation of a product with its security features, moving from security objectives to requirements, on to security specifications, and then to the implementation of the security features along with the rest of the product. The security requirements are stated as much as possible in the context of known security functional requirements from the criteria, amplified as necessary to be product implementation specific. There are a variety of assurance criteria-driven deliverables produced during the development process that help provide confidence in the correctness of product implementation against the functional requirements.

After development, the completed IT security product is subjected to a series of evaluator actions, also specified in the criteria, to validate the correctness of implementation and to determine the effectiveness of the product in meeting the security threats and policies that are the basis for the requirements.

Finally, there is a series of actions by some authoritative body (currently governmental) to review the case made by the evaluators that the product indeed meets a valid set of requirements and implementation specifications. This process is called 'certification of results' and is generally followed by entry of the product onto an approved list of evaluted products available for user procurement guidance.

A Brief History of IT Security Criteria:

The history of IT security criteria is rather complex (see Figure 4). The salient elements relate first to the growth in national initiatives, followed by growing recognition of the inutility of individual national action, which was then succeeded by a number of joint efforts that have culminated in the Common Criteria and its acceptance into the process of becoming an International Standard.

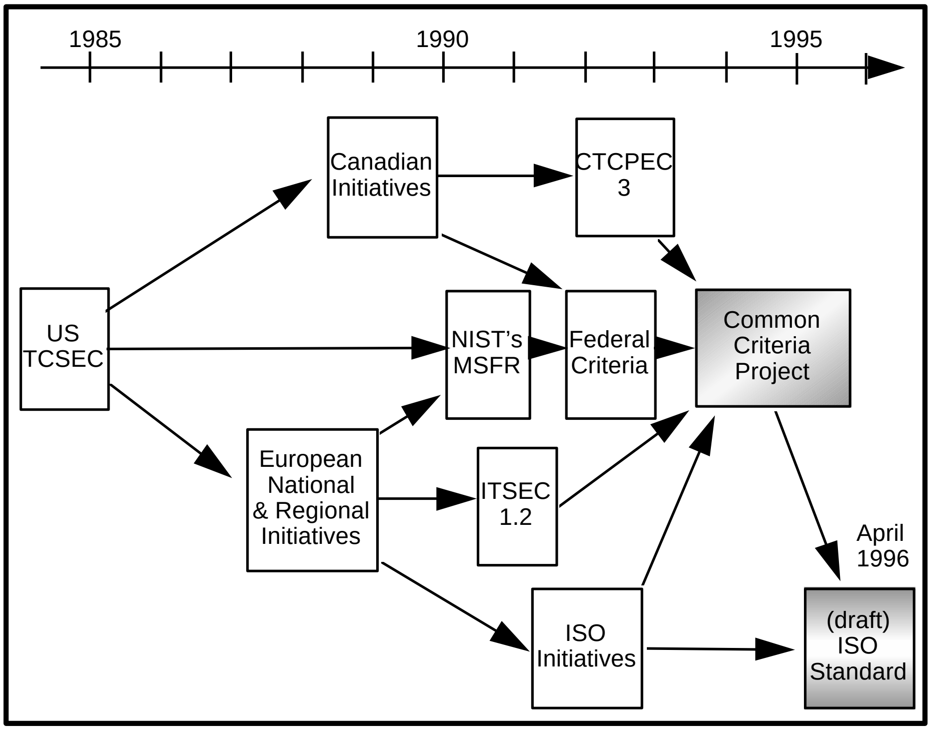

Figure 4: Brief History of IT Security Criteria

1. The first IT security criteria was the TCSEC, the fabled 'Orange Book', first published by the US National Security Agency (NSA) in 1983 based on earlier work done in conjunction with the National Bureau of Standards. This volume was fixed in form and application, and oriented towards multi-user operating systems without external connectivity. The TCSEC was very good for its time, and despite its requirement-set inflexibility, its fundamental technical requirements continue to be used in later criteria, and have been carried forward into the CC. The TCSEC was subsequently “interpreted” for both networks and databases. It has formed the basis for NSA product evaluations to the present time.

2. Owing to the inflexibility of the TCSEC and to the need to set up their own trusted product evaluation programs, several European nations and Canada began their own

criteria development efforts in the late 1980’s. The Europeans rather quickly pooled their efforts after a number of unilateral forays. Initial versions of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) and the European Community's Information Technology Security Evaluation Criteria (ITSEC) came out in 1990.

3. The ITSEC was the initial impetus for the search for a truly international standard which was begun in late 1990 by a working group of the International Standards Organisation (ISO). That group is called Working Group 3 of ISO’s Subcommittee 27, and has been led from the beginning by Professor Svein Knapskog of the Norwegian University for Science and Technology.

4. In the United States, NSA and NIST agreed to jointly re-work the Orange Book to bring it up to date technically and to make its security requirement sets more broadly applicable to non-military IT products.

- The first US effort was the Minimum Security Functional Requirements (MSFR), an update of the TCSEC’s C2 requirements set with the goal of being more useful to private industry and civil government bodies. The MSFR was heavily influenced by the ITSEC's Security Target philosophy, which separated functional and assurance requirements and justified each against expected threats in the intended environment of use.
- The second US effort was the draft Federal Criteria (FC) version 1, published in early 1993. The FC was in turn influenced strongly by the MSFR work and by the CTCPEC. One of the Canadian authors of the latter was an active member of the FC working group.

In 1993, the US and Canada agreed to harmonise their criteria, based on the draft FC and the newest version of the CTCPEC. They jointly announced these plans to the European Community, a decision was then made to pool North American and European criteria development efforts, and the Common Criteria (CC) effort was thereby born. That agreement was the first of the breakthroughs referred to in the title of this paper. This new project held promise to lead to the greater breakthrough everyone was hoping for -- the collapse of all ongoing criteria efforts into a single international criteria. The goal was to harmonise the several criteria into one, which would then be turned over to ISO as a contribution to the international standard. In large part, that objective has been achieved in April 1996, when ISO/SC27/WG3 accepted Parts 1 through 3 of the CC trial version 1.0 as the basis for its further work. This occurrence is indeed the second and key breakthrough that was long sought by the IT security community.

Common Criteria Project Participants:

The four national security agencies of France, Germany, the Netherlands and the United Kingdom which authored the ITSEC joined with Canada, NSA and NIST to form the Common Criteria Editorial Board in mid-1993. Initial plans were highly optimistic, envisioning that the several criteria involved could be 'aligned' in six months of hard work. In fact, it has taken over four times that long, due to the work required to resolve many fundamental differences in viewpoint. Trial-use version 1.0 of the Common Criteria was published in late January 1996, after two previous widely-reviewed draft versions. It is envisioned that after one year of application by the project participants and others, a new version 2 will be completed and handed over to ISO, and the criteria part of the project will be completed. There are other aspects of the CC Project which will continue on; these will be addressed shortly.

Overview of the Common Criteria Structure:

The CC consists of three major parts, following the original ISO criteria structure.

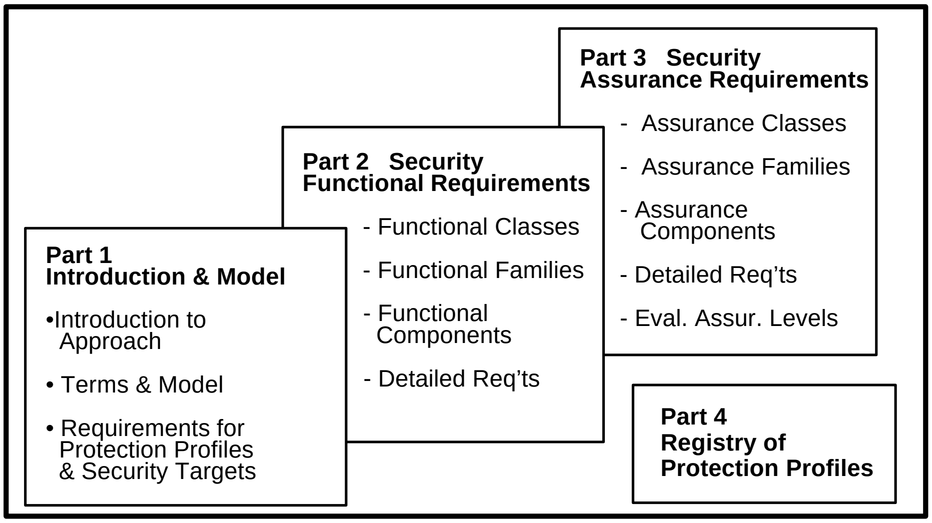

Figure 5: Common Criteria Structure

Part 1 consists of the introduction and presentation of the general model and concepts of IT security evaluation. Additionally, Part 1 includes normative requirements for the structure and content of the two constructs for stating requirements specified in the CC. These are the Protection Profile and Security Target, which will be described more fully later.

Part 2 is the catalogue of functional requirements. The attempt here has been, in the words of one of the CC principal authors, to write down everything we know about IT security functions and can evaluate. These security functions are grouped at a very high level into ten broad classes, each of which contains a number of families of related indivisible functional requirement components. The notion is that there should be very few unique and typically new security requirements at the level of "function" (more abstract than product-specific implementing mechanism) which are not covered by the catalogue, although some slow evolution is anticipated. It is expected that most seemingly unique security requirements will in fact be variants of the known functional requirement components in Part 2, and they can be stated through refinement of those component requirements to be more specific or detailed as needed.

Part 3 is the catalogue of assurance requirements, consisting of a set of discrete assurance components similarly to Part 2, plus a grouping of selected components into a series of seven increasingly rigourous packages called Evaluation Assurance Levels (EALs). The source criteria all have used variants of these levels in order to gauge the amount of assurance to be provided about an IT security product. Part 3 also contains evaluation criteria for Protection Profiles (PPs) and Security Targets (STs).

A new Part 4 is the initial registry of predefined PPs. It is anticipated that this document will be the precursor for a wider PP registration effort, possibly conducted by ISO. In the summer of 1996, ISO/SC27/WG3 undertook a new work item to develop a registry and registration procedures for PPs, that is expected to pave the way for this wider effort.

Protection Profile and Security Target:

The PP and ST constructs for specifying requirements for IT security products or systems have similar structures and numerous common elements.

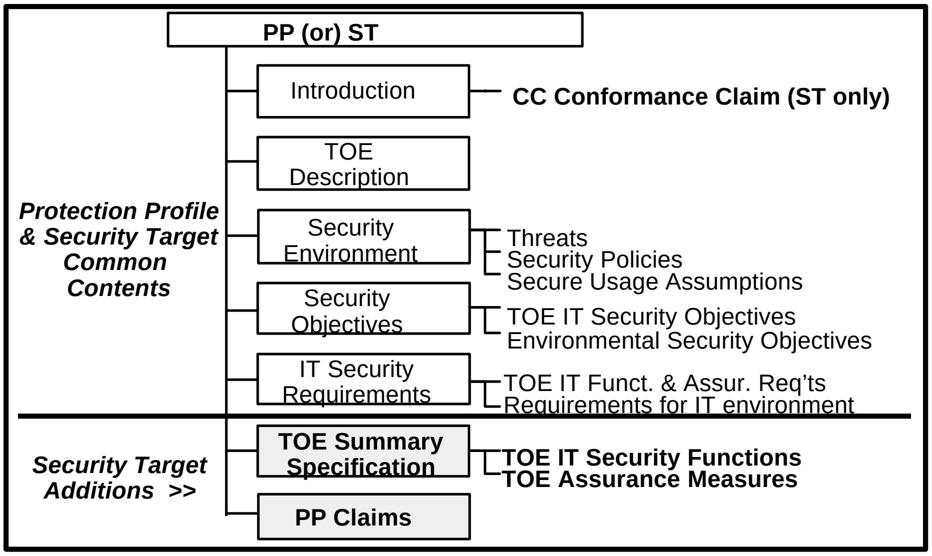
PP (or) ST
Introduction
CC Conformance Claim (ST only)
TOE Description
Protection Profile & Security Target Common Contents
Security Environment
Threats
Security Policies
Secure Usage Assumptions
Security Objectives
TOE IT Security Objectives
Environmental Security Objectives
IT Security Requirements
TOE IT Funct. & Assur. Req'ts
Requirements for IT environment
Security Target Additions >>
TOE Summary Specification
TOE IT Security Functions
TOE Assurance Measures
PP Claims

Figure 6: Protection Profile and Security Target Structure

Although they have much commonality, the PP and ST differ in two important respects:

- General versus specific product/system orientation -- The PP is intended to state a more general set of requirements that any of a number of IT security products or systems might fulfill. The ST is a specific requirement set for a single product or system (called Target of Evaluation or TOE in the CC).

- Detail of structure -- The PP and ST have common content down through the level of security requirements which are based on security objectives, which in turn are derived from statements about threats and security policies. The ST, covering a specific product or TOE, will go further. It is anticipated that STs typically will be formed from known and evaluated PPs in order to meet market requirements, but will amplify the requirements by containing detailed specifications for one single TOE or product. In such cases, the ST will also provide a claim of conformance of its TOE to a certain PP along with statements justifying that conformance.

It is expected that both the PP and ST will be formally evaluated, applying the criteria for them given in Part 3. This evaluation will make sure that security objectives to be met flow logically from the stated threats and security policies to be addressed, and that security requirements (both functional and assurance) fully cover the objectives. The PP is to be evaluated prior to its being registered for general use. The ST is to be evaluated in the first phase of the evaluation of the TOE which it describes and specifies.

Part 2 Functional Security Requirements - Classes:

Part 2 contains nine agreed classes or major groupings of specifiable IT security functional requirement components.

FAU -- Security Audit (35)
FCO -- Communication (Non-Repudiation) (4)
FCS -- Cryptographic Support *(in version 2)* (40)
FDP -- User Data Protection (46)
FIA -- Identification & Authentication (27)
FPR -- Privacy (Anonymity, etc.) (8)
FPT -- Protection of Trusted Security Functions (43)
FRU -- Resource Utilisation (8)
FTA -- TOE Access (11)
FTP -- Trusted Path (2)

Figure 7: Classes of CC Security Functional Requirements

These classes cover the known range of IT security functions. They are further subdivided into 75 families of 184 related components. Additionally, there is one draft Cryptographic Support class consisting of 15 families and 40 components that has been proposed and has been published with the CC version 1, but has not yet been agreed for inclusion in the CC.

The CC and Crypto

Because of the extreme sensitivity of the topic of crypto-algorithmic strength estimations, the CC project participants decided not to include requirements for assessment of the mathematical properties of algorithms in the criteria itself. It is assumed in CC evaluations that, when required for a particular product, some other entity will make the appropriate algorithmic assessment and then provide the results to the evaluators expressed in terms of “strength of function”.

It is recognised and agreed by the CC project participants that cryptographic administration and application need to be covered in the CC, especially to cover the security challenge posed by distributed systems and networks in general. There is a general understanding, however, that crypto is fundamentally a mechanism, or implementation detail of more general functional requirements. The CC requirements in Parts 2 and 3 are not intended to go down to the level of mechanism implementation -- these details can be specified in a Security Target as detailed refinements of existing requirements. (For example, a requirement for authentication by smart-card algorithm is seen as simply a more-specific implementation of several security functional component requirements in the family FIA_UAU, User Authentication.) There is a counter-argument that cryptographic support is such an important topic in today’s environment that it should be covered in the CC anyway. During the trial-use period a joint working group of the CC project organisations will resolve this question for CC version 2.

Late in the development of the CC, too late for the participants to come to agreement on it, a set of draft material on crypto based on the first view was presented for inclusion. It was agreed that the material was to be saved for possible future use in version 2 by being placed into a Technical Report (TR) to accompany the CCv1.0 during the trial use and comment period. This TR covers various aspects of cryptographic implementation, administration and key management. The crypto TR is generally available with the CC for public review and comment.

Assurance Requirements -- Classes:

Part 3 contains nine classes of specifiable assurance components covering both the correctness of TOE development and implementation and the effectiveness of the TOE in meeting its stated security objectives.

ACM - Configuration Management
ADV - Development
ATE - Tests
AVA - Vulnerability Assessment
ADO - Delivery and Operation
AGD - Guidance Documents
ALC - Life-cycle Support

APE - Protection Profile Evaluation
ASE - Security Target Evaluation

Figure 8: Classes of CC Assurance Requirements

Useful combinations of assurance components are combined into the seven Evaluation Assurance Levels (EALs) included in Part 3, as discussed next. Individual assurance components are specifiable when needed to augment these EALs for particular product needs.

Evaluation Assurance Levels:

The seven EALs are increasingly-strong packages of mutually supportive components covering requirements from each of the classes which have been developed for normal use in PPs and STs.

Level EAL1 - (new)
The lowest level which should be considered for purposes of evaluation

Level EAL2 - (like C1 - E1)
Best that can be achieved without imposing some additional tasks on a developer

Level EAL3 - (like C2 - E2)
Allows a conscientious developer to benefit from positive security engineering design without alteration of existing reasonably sound development practices

Level EAL4 - (like B1 - E3)
The best that can be achieved without significant alteration of current good development practices.

Level EAL5 - (like B2 - E4)
The best achievable via pre-planned, good quality, careful security-aware development without unduly expensive practices.

Level EAL6 - (like B3 - E5)
A “high tech” level for (mainly military) use in environments with *significant* threats and moderately valued assets.

Level EAL7 - (like A1 - E6)
The greatest amount of evaluation assurance attainable whilst remaining in the real world for real products. EAL7 is at the limits of the current technology.

Figure 9: CC Evaluation Assurance Levels (EALs)

The EALs cover a broad range of assurance, from simple verification of minimal development requirements (EAL1) to the full formalisation of theorem-proving applied against mathematical models of the TOE's functions (EAL7). As might be anticipated, the normal range of assurance for commercial IT security products is in the lower middle (EAL3 and EAL4), which are achievable by a conscientious developer using sound engineering and good commercial development practices. EAL3 is intended to be comparable to the assurance requirements in the TCSEC’s C2.

Part 4 -- Registry of Predefined Protection Profiles:

A central part of the CC notion is the Protection Profile. Well-crafted PPs for products with wide usefulness, expressed in terms of known and widely accepted functional and assurance requirement statements in the CC, are the goal. Part 4 is intended primarily as an initial set of PP examples and a stimulus for development of other PPs. The current version of Part 4 includes three PPs, two commercially-oriented ones from previous criteria (CS1/C2 and CS3) and a new low-end firewall (filtering packet router). Ultimately, it is envisioned that there will be a living catalog or registry of PPs. To that end, there were already at least 20 projects underway by Summer 1996 to develop various kinds of PPs against the CC.

The Future: Trial Use Period and Follow-On Tasks:

Now that CC version 1 is available to all and its ISO acceptance is a reality, it will be useful to look to the follow-on phases of the project, most of which have already begun. The project sponsors have entered into a one-year trial-use period for CCv1, in which it is being tested and built upon for practical use. The following implementation activities are under way:

- A significant number of trial evaluations are either planned or already initiated in the participating nations. These early evaluations are mainly comparisons, in which a product is evaluated against both the existing criteria and the new CC. The evaluators are expected thereby to grow in confidence that a CC-based evaluation will produce a predictably acceptable result.
- A major part of the current activities is dedicated to developing a common evaluation methods manual. This is a major activity which is one of the key underpinnings for all later CC-based work, especially the following.
- Preliminary work has begun on exploring the basis for mutual recognition of evaluations between North America and Europe. The three legs supporting mutual recognition are a stable and common criteria, common methods for their application, and mutual expectations of similar competence of the evaluators.
- The project sponsors are actively soliciting comments from the international IT security community on the CC version 1. Comments will be received until the end of October 1996. Directions for formatting and submitting comments are in each of the CC volumes. The CC has been made available both electronically on project participant internet websites (visit NIST’s site: http://csrc.nist.gov/nistpubs/cc) and on CD-ROM that is free upon request from any of the participants.

- It is anticipated that CC version 2 will be developed during 1997, based on all the feedback gathered from the trials, the comments and other related work going on during this year. This definitive version will represent the end of the criteria-development phase of the project. At that point, the CC will be fully relinquished to ISO for completion as an international standard.
- Later on, it is envisioned that implementing guidance, like that published to accompany the Orange Book, will be needed. There is already a proposal in ISO to begin work on the first volume, guidance on preparation of Protection Profiles and Security Targets.
- As development and evaluation of globally-acceptable Protection Profiles is a major goal of the project, procedures for their international registration are required. At the present time, ISO's new work item holds significant promise to develop those registration procedures.

Summary:

The results of the Common Criteria project can indeed be viewed as a major breakthrough in the field of IT security. For the first time, six nations, representing both the military interests as well as civil government and private industry, have not only sat down at the table to iron out their philosophical differences in IT security but have achieved a great measure of accord. Admittedly, this accord not been won easily; it has come at a significant expense of both time and energy. Notwithstanding, the result is a very flexible and extensible approach that is designed to meet the needs of today and tomorrow; indeed the CC is the next generation criteria.

In doing so, the developers of the new CC have been careful to protect the fundamental technical principles of IT security, such as the Trusted Computing Base and Reference Mediation on the one side and effectiveness and correctness on the other. The resulting approach represented by the CC version 1 is a major contribution to international harmonisation. The fact that it has already been accepted by ISO as the basis for further work towards an international standard is indicative of the success of the project.

The desired end-state is now in sight -- a level playing field for IT security products world-wide, where it should make no difference to the consumer where a product is manufactured or evaluated. The degree of trust to be placed in a product's secure and predictable operation will be known and accepted.